Available online at www.sciencedirect.com

ScienceDirect

Procedia Manufacturing 3 (2015) 1066 – 1073

Procedia MANUFACTURING

6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences, AHFE 2015

Mindlessness attacks

Feng Zhu[a,*], Sandra Carpenter[b], Swapna Kolimi[a]

[a]*Department of Computer Science, The University of Alabama in Huntsville, Huntsville, Alabama, USA*
[b]*Department of Psychology, The University of Alabama in Huntsville, Huntsville, Alabama, USA*

Abstract

In our daily life, we complete many tasks without paying much attention and thinking actively. We have the tendency to be in this automatic cognitive state, which is known as mindlessness. Mindlessness can occur in interpersonal communication and can even occur when people interact with computers. We identify that mindlessness may be used as an attack. A website, for example, may exploit mindless behavior and acquire personal identity information. In our experiment, we designed a car insurance website that requested participants to provide their identity information. The mindlessness attacks successfully acquired identity information from more participants than the control condition. To the best of our knowledge, this is the first experimental study of mindlessness attacks in personal information requests.

Keywords: Mindlessness; Psychology; Identity management; Security; Privacy

1. Introduction

"Excuse me, may I use the Xerox machine because …?" It was an experiment that psychologists Langer, Bland, and Chanowitz conducted in front of a copy machine at their university [1]. The experimenters tried to get in front of a person who wanted to make a copy. They found that it did not matter whether the reason was sound ("because I am in a rush") or not ("because I want to make a copy"); people were equally likely to offer the favor. But if the request was not followed by a reason, they found that people were less likely to comply.

* Corresponding author. Tel.: 1-256-824-6255; fax: 1-256-6239.
E-mail address: fz0001@uah.edu

doi:10.1016/j.promfg.2015.07.174

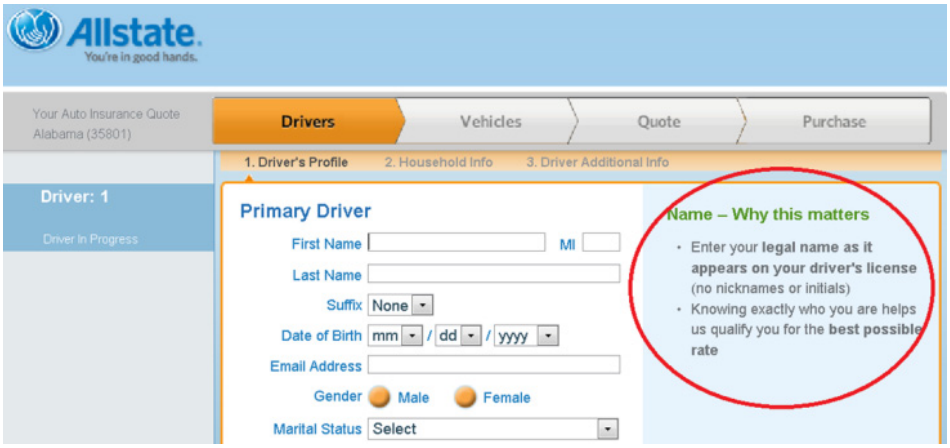

Fig. 1. A screenshot of an Allstate car insurance web page from 2011.

Complying with the request in the above scenario was considered a mindless behavior [1]. In interpersonal communication, one may mindlessly respond to sentence structures instead of the actual contents. Perhaps, the mindlessness behavior may happen when people interact with computers.

Allstate Insurance Company's car insurance website provided reasons why customers should provide their identity information. When a field was clicked or the mouse cursor was hovered over the field, a reason was displayed as shown in Figure 1. Many of the reasons do not seem to be sound. (Allstate's car insurance website was redesigned and the reasons are not currently provided.) This could be considered a mindlessness attack, and it provided a template and scenario for our mindlessness attack research. We wanted to study how much more likely people were willing to provide their private information under mindlessness conditions.

Westin's survey results have indicated that most people worry about their privacy (e.g., general privacy [2] and medical information [3]). Our previous research studied people's attitudes towards keeping 26 identity elements private. It indicated that most people want to keep their sensitive identity information private [4].

Studies have shown that more than 90% of commercial websites collect identity information [5]. Names, email addresses, home addresses, and phone numbers are the most common identity elements collected. Besides the identity information that can uniquely identify individuals, service providers collect additional information from users based on their interests. For example, health related websites, often sponsored by pharmaceutical companies, collect a great deal of medical information [6].

Anderson warned in his textbook that real attacks exploit psychology at least as much as technology [7]. In our research, we studied whether people behave mindlessly when unsound reasons are given for requesting personal identity information, by investigating the influence of a mindlessness attack on disclosure of identity information.

We developed websites that provided "car insurance quotes" and also registered domain names for the sites. There were 45 people who participated in the mindlessness attack study. Our experiment showed that participants were more likely to provide identity information under the mindlessness attack condition. For instance, they were 4 times more likely to provide driver license numbers than participants in the control (no attack) condition.

Our key contribution is that the framing of personal information requests, inducing mindlessness, may be used as an attack. To the best of our knowledge, this is the first experimental study using a sentence structure on mindlessness as an attack. Our experiments show that mindlessness attacks may be effective to acquire people's identity information.

The rest of the paper is structured as follows. We first discuss background and related work. Then, we describe the experimental design, method, key findings, and participants of the mindlessness attacks. Last, we outline our future work and our contributions.

2. Background and related work

In this section, we provide more background information about mindlessness behaviors, identity exposure attitudes and behaviors, and psychological attacks on private information.

2.1. Mindlessness and psychological studies

Mindlessness occurs in a great deal of our daily behaviors. It is an automatic mode in which people complete their tasks [8-9]. In this mode, we do not consciously pay attention to our behaviors. These automatic behaviors may be simple motor acts, or even complex and intelligent acts, such as reading and writing [10].

Mindlessness and its counterpart, mindfulness, are a dimension of our cognitive functioning and physiological functioning [11]. In the mindless state, one does not attend to new signals and information in the current context, but relies on old categories, and acts from a single perspective [8].

Studies have analyzed whether the degree of mindlessness in people differs with social variables such as moods and familiarity with tasks [12-14]. In general, people who are in a happy mood tend to process information by relying on general knowledge structures, which has a high correlation with performing a task at hand mindlessly. Another set of studies has indicated that familiarity with a certain task leads to the person being confident in their ability to repeat the task [15-16]. People "think" that they can perform the task more than adequately, which leads to the task being done in a mindless way.

When interacting with computers, people also mindlessly apply social rules and expectations. In Nass and Moon's studies [17], participants showed the same perceptions of gender stereotypes, ethnicity, and loyalty to groups in the human computer context. Their studies further showed that mindlessness is a deeply ingrained behavior because of over-learning (leading to automatic behavior). Participants in this research applied social rules to computers.

2.2. Identity exposure attitudes and behaviors

People in general worry about their privacy [2]. But several studies have shown that many people provide sensitive information such their income, investments, home addresses, etc. on the Internet without a reason [18-19]. Our research also showed that people's identity exposure behaviors did not necessarily match their attitudes [4].

We surveyed people's privacy attitudes towards protecting 26 identity elements [4]. For some identity elements, everyone considered those to be very important to keep private (e.g., driver's license number). Some elements (e.g., favorite TV programs) were considered by everyone as not at all important to keep private. In addition, there are identity elements that some people considered important to keep private, while others did not think the same. In this mindlessness research, we selected six identity elements that at least many people think are important to keep private.

2.3. Attacks based on psychology

Many computer security and privacy attacks are based on psychology [7]. For example, social engineering attacks, such as social phishing, target Internet users and are widespread [20-21]. They are based on the psychological manipulation of victims for either a short period of time or an extended period of time. While some attacks have been studied in the recent years [22-23], many new types are expected to be invented [23-24].

There are few studies on peoples' identity exposure behaviors under psychological attacks and mitigations. Some of our previous research showed that reciprocity, a social norm that people take turns sharing personal information, may be used to effectively acquire people's identity information [25]. Under the reciprocity attack condition, participants were 3 times more likely to expose their income information and 5 times more likely to expose their date of birth information.

Other research has shown that people are more willing to provide personal information if explanations of privacy practices are explained effectively [26]. That is, informing people of how their information will be used increases

disclosure. The researchers built a website, ostensibly to recommend books on the basis of personal preferences. In this context they could request personal information in a realistic way. This research was conducted with the goal of better understanding how being transparent with privacy policies can increase data sharing and purchase behavior. The results, however, indicate that providing explanations for requests for personal information may be effectively used to increase disclosure of personal information. The current research builds on this foundation.

3. The mindlessness attack experiment

We hypothesized that participants in the mindlessness condition would provide more identity information than the participants in the control condition.

In our mindlessness attack study, we asked participants for their identity information and provided them reasons for requesting the information, which may not be sound reasons. We conducted the experiments and follow-up surveys. We wanted to understand identity exposure behaviors under mindlessness attack and control conditions. We wanted to analyze the impact of the mindlessness attacks on identity exposure behavior. We selected six identity elements that people consider very important or extremely important to keep private and that were also related to the car insurance context.

3.1. Participants

We recruited participants through courses in the psychology department. We asked students to find one or two volunteers (parents, guardians, and friends) who were 30 years of age or older. The students were given 1 activity point for each volunteer that participated in the study. We believed that with the age limitation our participants would have had several years of driving experience and some car insurance purchasing experience.

After a student found a volunteer, he or she emailed our lead researcher with the participant's name, age, and email address. Then, our researcher emailed the participants directly with the link to our experiment website. The two websites (mindlessness attack or control) were randomly assigned to the participants.

Our experiment was attended by total 45 people: 21 in the control condition and 24 in the mindlessness attack condition. Among the participants, 35.5% were male and 64.5% were female. The participants' ages ranged from 30 years of age to 65 years of age, with the average age being 46.5. The demographic information is as follows: 84.5% of them were White (not Hispanic), 15.5% were Black or African American. None of the participants reported being of Asian, Hispanic, or mixed heritage.

The procedures of this experiment (and the other two experiments discussed in this paper) were approved by our university's IRB.

3.2. Websites and scenario

We advertised the study as a beta test of a website for a car insurance company, which seemingly had collaborated with the university to recruit participants, without mentioning anything about our study of computer security and privacy.

We registered a domain name. The website was hosted by godaddy.com. We also purchased a SSL certificate, and thus the communication between a participant and the website was over HTTPS.

On the basis of what we learned from our previous computer security and privacy experiments, we wanted to reduce participants' perception that studies conducted by the university were safe because this led participants to provide all of the information requested [25]. One approach that had been useful in our previous study was to present a disclaimer in the beginning of the study. On the webpage, we introduced a third-party, Auto Needs insurance company, which ostensibly created the website and collected the data. In addition, we stated that the university merely conducted the experiments for the insurance company.

Participants accessed the website on the Internet and completed the study at their convenience. Nevertheless, we wanted participants to focus on the study and progress through the whole website and survey without breaks. A session would expire if a participant left the website unattended for an extended time period. In a separate email that we sent to the participants, we reminded them to complete their interaction with the website study in one sitting.

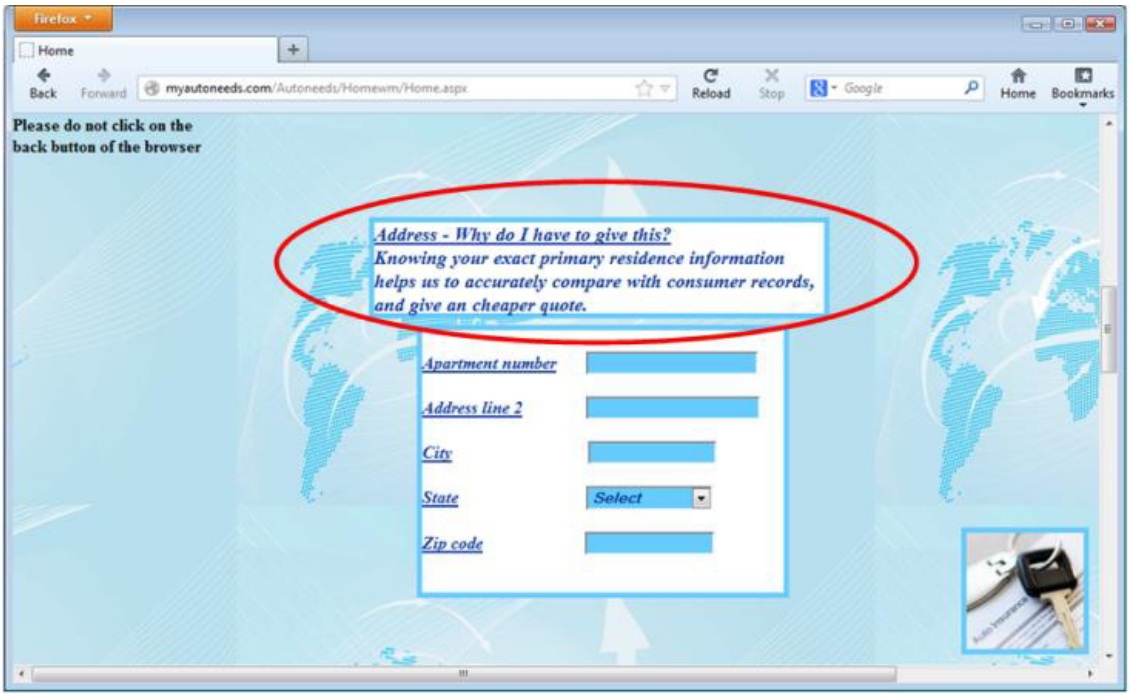

Fig. 2. Screenshot of a mindlessness attack.

We used a mixed-method design to study participants' identity exposure behavior and their privacy rationale. In the first part of the study, we presented the car insurance websites. The second part requested feedback about the quality of the website.

For the first part, the websites requested that participants provide the type of information that is typical of commercial car insurance companies' websites. They included six sections: driver's information, insurance history, vehicle information, accidents and violation history, vehicle conditions and existing damages, and a quote for their car insurance. Participants were asked to use the website, then evaluate its usability in accessing an immediate online auto insurance quote.

We designed two versions of the car insurance website: the mindlessness attack condition website and the control condition website. The two websites looked very similar. They both had the same graphics, fonts, forms to request identity information, and order of the pages. The only difference was that in the mindlessness attack condition reasons were given (why participants should provide their identity information) as shown in Figure 2.

We did not actually collect participants' identity information or their other car insurance related information. Instead, we only recorded whether they provided information or not. Thus, their identity information was not transmitted over the Internet to the web server. As computer security and privacy researchers, we wanted to protect participants' private information and not collect their information.

In the feedback part of the study, we asked participants whether they had given their identity information to the car insurance website, whether they falsified the identity elements, or whether they only gave partial information. In this way, we knew the participants' identity disclosure behaviors. That is, we could assess whether the participant had "faked" any of the information they had provided and, if so, why. In addition, we requested that participants provide demographic information and general opinion of the websites and asked them to rate the importance of the identity elements.

After we completed the experiments, we emailed participants and debriefed them about the study. We explained that our goal in this research project was to understand identify exposure behaviors in the mindlessness and control conditions. We told them that their identity information was not collected and that the car insurance website was merely a way to attempt to collect identity information.

3.3. Mindlessness attacks

The insurance websites requested that participants provide 24 pieces of information related to the car insurance quote. We provided reasons for all requested information. Among these pieces of information, we were particularly interested in the following identity elements: email address, driver's license number, date of birth, phone number, home address, and zip code. Table 1 shows the identity elements and reasons given for requesting the identity information. All requests started with: Why do I have to give this? Then, one or more reasons were given. For some elements, we grouped the messages together (e.g., home address and zip code).

For many of these reasons provided, we mimic the reasons that were provided at the Allstate website. For other reasons, such as the ones used for email address and phone number, one may find that they are similar to the reasons used by other websites and stores.

Table 1. Six identity elements and the reasons that were given for requesting information in the mindlessness experiment.

Identity elements	Reasons: Why do I have to give this?
Date of birth	Age is one of the many factors that may influence your rates.
Driver's license number	A long history of insurance coverage with no gaps may mean lower rates. If you were insured on someone else's policy, we count that as a part of your insurance history details.
Email address	You will receive an electronic copy of your quote, and we will not share your email address with any other companies and organizations.
Phone number	We may use it to look up your quote when you call us or use your phone number to contact you about a quote you started or received.
Home address & Zip code	Knowing your exact primary residence information helps us to accurately compare with consumer records, and give a cheaper quote.

The reason given for requesting the participants' date of birth might sound logical, but date of birth is much more precise than one's age, which is all that is really needed for a car insurance quote. Similarly, home address and zip code are also specific information that can uniquely identify individuals. Giving this of information, however, may not guarantee that one will receive a cheaper or more accurate immediate online quote.

While some reasons might be sound, others may not be reasonable or even related. For example, there was no specific reason given for requesting the driver's license number. The driver's license number field was grouped with the insurance history. The two reasons that provided were only related to one's insurance history.

Table 2. Number and percentages of participants providing identity information. * Asterisks indicate the percentage is significantly larger than the control group (p-value < 0.05).

Identity elements	Control condition (21 participants)		Mindlessness attack condition (24 participants)	
Date of birth	16	76%	22	91%
Driver's license number	9	43%	18	75%*
Email address	16	76%	24	100%*
Phone number	15	71%	19	79%
Home address	16	76%	21	88%
Zip code	20	95%	20	83%

3.4. Results and analysis

Whether more participants provided personal information in the mindlessness attack condition was the dependent variable of interest. If participants did not enter any information into the request text box, this was considered non-disclosure. If participants did input information, we reviewed their responses to the post-website questionnaire that asked them whether they had faked any information while interacting with the website.

Overall, participants in the mindlessness condition exposed more information than participants in the control condition except for the zip code, as shown in Table 2. Driver's license numbers were exposed the least, while other elements were exposed at a similar level. Such behaviors partially match our survey data, in that people think a driver's license number is one of the most important identity elements to keep private and that the other five elements are considered similarly important to keep private [4].

The mindlessness version of the website successfully collected 75% of the participants' drivers' license numbers, whereas in the control condition only 43% of the participants shared their correct driver's license numbers. Thus, the attack proved to be effective (Z-value = -2.30 and p-value = 0.011), as indicated by a Z-test comparing the proportions in the two conditions. The odds ratio that measures the influence of mindlessness attack was 4. That is, the odds of exposing the driver's license number under the mindlessness attack were four times greater than for the participants who were not under the attack.

The mindlessness attack also successfully collected email addresses from participants. All participants in the attack condition provided the information, whereas 72% of the participants in the control condition did so. It was also statistically significant (Z-value = -2.56 and p-value = 0.005). Since all participants provided email addresses in the mindlessness condition, the odds ratio approaches infinity. If the sample size were larger than what we had, there would likely be participants who did not provide the information. The odds ratio, in such a case, would be still large. That is, participants were highly likely to provide their email addresses.

Although more participants gave their phone numbers in the mindlessness condition compared to the control condition (71% vs. 79%), the increase was not statistically significant. Similarly, in a separate study [25], participants were not more likely under a reciprocity attack to provide their phone numbers. Perhaps participants more frequently provide phone number information, since they are often asked for their phone numbers at checkout registers in stores. Participants who did not want to provide phone numbers frequently indicated, in the later survey, that they did not want to receive marketing calls.

The differences of exposure for the other three identity elements – date of birth, address, and zip code – were not statistically significant across conditions. In this scenario, participants in the control condition exposed their identity information at a much more higher level than people's general attitudes towards keeping these elements private [4].

4. Conclusion and future work

We identified that people's mindless behaviors may be maliciously exploited. Our major goal in this research was to verify that a mindlessness attack may effectively acquire people's private identity information. Our experiment showed that by giving reasons for requesting information, more participants provided their identity information. An unsound reason or even an unrelated reason may cause participants to expose more information. The mindlessness attack experiment was successful on some identity elements (email address and driver's license number) and failed on others (date of birth, phone number, home address, and zip code). More research is needed to identify the relationships among the soundness of the mindlessness attack messages, the context, and the identity elements.

Our study has a few limitations. First, as a computer security and privacy study, we wanted to learn participants' behaviors and wanted to protect their privacy by not actually collecting their information. We relied on their honest responses and accurate recall of their accurate disclosure or information faking behaviors in the feedback section. Second, although we used a disclaimer and designed and deployed the websites that looked like a third-party was running them, several participants still stated in the feedback survey that they trusted university experiments and felt comfortable providing their information. If participants paid attention to the consent form, they would notice that there would be no harm to them and thus they might behave less cautiously.

One of our ongoing research goals is to design mitigation approaches. We based our design on research of warnings. We tested warning messages with signal words and short messages. Specifically, we use the C-HIP model of information processing [27] as an investigative tool to determine the reasons why some warnings are successful and others are not, and why some warnings are more effective.

Acknowledgements

This work is supported by the National Science Foundation, under grant 1220026 and grant 1043945.

References

[1] E. Langer, et al., "The mindlessness of ostensibly thoughtful action: The role of "placebic" information in interpersonal interaction," Journal of Personality and Social Psychology, vol. 36, pp. 635-642 1978.
[2] A. Westin, "1994 Equifax/Harris Consumer Privacy Survey," 1994.
[3] P. Kumaraguru and L. F. Cranor, "Privacy Indexes: A Survey of Westin's Studies," Carnegie Mellon University2005.
[4] F. Zhu, et al., "Understanding Identity Exposure in Pervasive Computing Environments," Pervasive and Mobile Computing, vol. 8, pp. 777-794, 2012.
[5] M. Culnan, "Protecting Privacy Online: Is Self-Regulation Working?," Journal of Public Policy & Marketing, vol. 19, pp. 20-26, 2000.
[6] K. B. Sheehan, "In Poor Health: An Assessment of Privacy Policies at Direct-to-Consumer Web Sites," American Marketing Association, vol. 24, pp. 273-283, 2005.
[7] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition: Wiley, 2008.
[8] E. Langer, The Power of Mindful Learning: Da Capo Press, 1998.
[9] E. Langer, Mindfulness: Da Capo Press, 1989.
[10] L. M. Solomons and G. Stein, "Normal Motor Automation," Psychological Review, vol. 36, pp. 492-512, 1896.
[11] E. Langer, "Matters of Mind: Mindfulness/Mindlessness in Perspective," Consciosness and Cognition, vol. 1, pp. 289-305, 1992
[12] H. Bless, and Clore, G.L., "Mood and the Use of Scripts: Does a happy Mood Really Lead to Mindlessness?," Journal of Personality and Social Psychology, vol. 71, pp. 665-679, 1996.
[13] D. Johnson, and Gardner, J., "Exploring mindlessness as an explanation for the media equation: a study of stereotyping in computer tutorials," Personal and Ubiquitous Computing, vol. 13, pp. 151-163, 2009.
[14] N. Schwarz, and Bless, H., "Happy and mindless, but sad and smart? The impact of affective states on analytic reasoning," in Emotion and social judgements, J. Forgas, Ed., ed Elmsford, NY, US: Pergamon Press, 1991, pp. 55-71.
[15] E. J. Langer, Mindfulness: Choice and Control in Everyday Life. London: Collins-Harvill, 1991.
[16] E. J. Langer, On Becoming an Artist: Reinventing Yourself Through Mindful Creativity: Random House Digital, Inc., 2005.
[17] C. Nass and Y. Moon, "Machines and Mindlessness: Social Responses to Computers," Journal of Social Issues, vol. 56, pp. 81-103, 2000.
[18] M. S. Ackerman, et al., "Privacy in E-Commerce: Examining User Scenarios and Privacy Preference," in Proceedings of the 1st ACM conference on Electronic commerce, Denver, Colorado, 1999.
[19] S. Spiekermann, et al., "E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus actual Behavior," in Proceedings of the 3rd ACM conference on Electronic Commerce, Tampa, Florida, 2001.
[20] C. F. M. Foozy, et al., "Generic Taxonomy of Social Engineering Attack," presented at the Malaysian Technical Universities International Conference on Engineering & Technology (MUiCET 2011), Batu Pahat, Malaysia, 2011.
[21] T. N. Jagatic, Johnson, N.A., Jakobsson, M., and Menczer, F. (2007) Social Phishing. Communications of the ACM.
[22]J.Goodchild. (2012, Social Engineering: The Basics. CS Online: Data Protection. Available: http://www.csoonline.com/article/514063/social-engineering-the-basics
[23] B. Böck, Klemen, M. D., and Weippl, E. R., "Social Engineering," in Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications. vol. 3, H. Bidgoli, Ed., ed Hoboken, NJ, USA: John Wiley & Sons, 2007.
[24] S. Granger. (2001, Social Engineering Fundamentals, Part I: Hacker Tactics.
[25] F. Zhu, et al., "Reciprocity Attacks," in Symposium On Usable Privacy and Security, Pittsburgh, PA, 2011.
[26] A. Kobsa and M. Teltzrow, "Contextualized Communication of Privacy Practices and Personalization Benefits: Impacts on Users' Data Sharing and Purchase Behavior. ," in Fourth International Workshop, PET 2004,, Toronto, Canada., 2005, pp. 329-343.
[27] M. S. Wogalter, "Communication-Human information processing (C-HIP) model," in Handbook of Warnings, M. S. Wogalter, Ed., ed, 2006.